Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A method for secure data transmission between a first subscriber and second subscribers, the first subscriber being a tachograph in a commercial vehicle and the second ~~subscriber~~ subscribers being memory cards having at least one respective data store, wherein the first subscriber has a memory which stores a particular number of entries each comprising identifiers and associated security certificates from second subscribers with a detection time for the security certificate, the method comprising the steps of:

fetching an identifier by the first subscriber from ~~the~~ a connected second subscriber of the second subscribers, the connected second subscriber being connected to the first subscriber;

comparing by the first subscriber the fetched identifier with the identifiers stored in the memory[[,]];

if a matching identifier is present, prompting the security certificate associated with the identifier to be a basis for a subsequent data transmission and updating the detection time for the security certificate to a current system time[[,]]; and

if no matching identifier is stored in the memory, prompting the first subscriber to perform security certificate verification with the connected second subscriber and, in the event of verification, storing an entry corresponding to the verified security certificate with a current detection time in the memory, with the entry with the oldest detection date being replaced by the new entry if a particular number of entries has already been reached.

2. (Currently Amended) The method according to claim 1, wherein the identifier is a public key from an RSA method from the connected second subscriber.

3. (Currently Amended) The method according to claim 1, wherein a subsequent data transmission is effected in ~~TDES encypted~~ TDES-encrypted form, with verification of the security certificates being followed by both subscribers sending a random number in encrypted form to the other subscriber and both subscribers independently of one another each using the two random numbers to determine a common key for date transmission using the same algorithm.

4. (Currently Amended) The method according to claim 1, wherein the verification of the security certificate from the first subscriber by the connected second subscriber and vice versa comprises the following n number of steps:

in a first step, the connected second subscriber sends the first subscriber a first security certificate which the connected second subscriber subjects to verification using a first public key and in so doing ascertains a second public key, and if the verification results in authenticity then the first step is repeated (n-1) times using a further transmitted security certificate and the second public key ascertained in the previous step instead of the first public key, with a new second public key and a verification result always being obtained.

5. (Currently Amended) The method according to claim [[1]]4, wherein n=3.